

**REMARKS**

This Application has been carefully reviewed in light of the Office Action mailed October 3, 2005. Applicant appreciates the Examiner's consideration of the Application. Claims 1-2, 7-12, and 17-18 have been amended to clarify, more particularly point out, and more distinctly claim inventive concepts previously present in these claims. Certain amendments do not narrow the scope of the claims, and certain amendments are not required for patentability. Applicant respectfully submits that no new matter has been added by the amendments to the claims. In order to advance prosecution of this Application, Applicant has responded to each notation by the Examiner. Applicant respectfully requests reconsideration and favorable action in this case.

**Section 103 Rejection**

The Examiner rejects Claims 1-18 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,357,008 to Nachenburg ("*Nachenburg*") in view of U.S. Patent No. 6,453,345 to Trcka ("*Trcka*"). Applicant respectfully traverses this rejection for the reasons discussed below.

Applicant respectfully submits that the combination of *Nachenburg* and *Trcka* proposed by the Examiner fails to disclose, teach, or suggest the elements of Claims 1-18. For example, *Nachenburg-Trcka* combination fails to disclose, teach, or suggest the following elements recited Claim 2:

- (1) determining that one of the listed memory regions is larger than a predetermined size; and
- (2) triggering a viral detection in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code.

First, *Nachenburg* fails to disclose, teach, or suggest the element. *Nachenburg* discloses a method for detecting computer viruses. According to *Nachenburg*:

[The method comprises] three phases: a decryption phase, an exploration phase, and an evaluation phase. A purpose of the decryption phase is to emulate a sufficient number of instructions to allow an encrypted virus to decrypt its viral body. A purpose of the exploration phase is to emulate at least once all sections of code within a region deemed likely to contain any virus present in the target program. A purpose of the evaluation phase is to analyze

any suspicious behavior observed during the decryption and exploration phases to determine whether the target appears to be infected.

(*Nachenburg*, Abstract.) That is, suspicious behavior observed during the decryption and exploration phases is analyzed during the evaluation phase to determine whether the target appears to be infected. *Nachenburg* discloses a list of suspicious operations at column 9, lines 26-65.

Presumably, the system of *Nachenburg* would trigger an alarm after detecting suspicious behavior, but not in response to the size of a memory region. Accordingly, *Nachenburg* fails to disclose, teach, or suggest “determining that one of the listed memory regions is larger than a predetermined size,” and “triggering a viral detection in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code,” as recited Claim 2.

Second, *Trcka* fails to disclose, teach, or suggest the element. *Trcka* discloses an automated monitor application. According to *Trcka*:

The Automated Monitor application 140 uses known data processing techniques (virus checking, transaction monitoring, etc.) to automatically check for and track suspect network events. In one configuration option, the Automated Monitor 140 checks all inbound transfers of executable files for known viruses. By selecting an ALERT MONITOR menu option on the graphical user interface 104, the user can enable and disable various visual and audible event alarms. For example, the user can configure the Automated Monitor 140 to trigger an audible or visual alarm upon detecting a virus in an inbound file transfer.

(*Trcka*, column 17, lines 24-34.) That is, *Trcka* merely discloses the triggering an alarm upon detecting a known virus. *Trcka*, however, fails to disclose, teach, or suggest “determining that one of the listed memory regions is larger than a predetermined size,” and “triggering a viral detection in response to determining that one of the listed memory regions is larger than the predetermined size, the viral detection alarm indicating detection of viral code,” as recited Claim 2.

Independent Claims 1, 7-12, and 17-18 recite certain limitations substantially similar to those recited in independent Claim 2. Accordingly, for at least the same reasons, Applicant also respectfully requests reconsideration and allowance of independent Claims 1-2, 7-12, and 17-18.

The dependent claims are allowable based on their dependence on the independent claims and further because they recite numerous additional patentable distinctions over the reference of the rejection. Moreover, Applicant traverses the Official Notice taken by the Examiner as to the rejection of Claims 5 and 15. Specifically, the Examiner states, "Regarding part a, *Nachenburg* ... does not specifically disclose a determination that the regions are contiguous. The examiner takes official notice that it would have been obvious to one of ordinary skill in the art at the time the invention was filed to also determine whether the memory regions are contiguous." (Office Action, page 4.)

"It is never appropriate to rely solely on 'common knowledge' in the art without evidentiary support in the record, as the principal evidence upon which a rejection was based." M.P.E.P. § 2144.03 (citing *Zurko*, 258 F.3d 1379, 1385, 59 U.S.P.Q.2d 1693, 1697 ("[T]he Board cannot simply reach conclusions based on its own understanding or experience-or on its assessment of what would be basic knowledge or common sense. Rather, the Board must point to some concrete evidence in the record in support of these findings"))).

"Official notice without documentary evidence to support an examiner's conclusion is permissible only in some circumstances. While 'official notice' may be relied on, these circumstances should be rare when an application is under final rejection or action under 37 CFR 1.113. Official notice unsupported by documentary evidence should only be taken by the examiner where the facts asserted to be well-known, or to be common knowledge in the art are capable of instant and unquestionable demonstration as being well-known. As noted by the court in *In re Ahlert*, 424 F.2d 1088, 1091, 165 USPQ 418, 420 (CCPA 1970), the notice of facts beyond the record which may be taken by the examiner must be 'capable of such instant and unquestionable demonstration as to defy dispute'" M.P.E.P. § 2144.03 (citing *In re Knapp Monarch Co.*, 296 F.2d 230, 132 U.S.P.Q. 6 (C.C.P.A. 1961)).

"It would not be appropriate for the examiner to take official notice of facts without citing a prior art reference where the facts asserted to be well known are not capable of instant and unquestionable demonstration as being well-known." M.P.E.P. § 2144.03 (emphasis in original).

Applicant disagrees with the Official Notice taken by the Examiner because it would not have been obvious to one of ordinary skill in the art at the time the invention was filed to modify *Nachenburg* to determine whether the memory regions are contiguous. *Nachenburg*

establishes whether a virus proper region has been set merely to determine whether to end a procedure:

In a first step 420, the decryption module 152 determines whether or not the virus proper region has already been set (i.e., during a prior performance of either a third step 424 or a sixth step 430 as discussed further below). If the region has already been set, then the tenth procedure 320 ends and the decryption module 152 loops back to the second procedure 304 of the decryption phase 252.

(*Nachenburg*, column 11, lines 36-42.) Accordingly, there is no need to determine whether regions are contiguous. Thus, it would not have been obvious to one of ordinary skill in the art at the time the invention was filed to modify *Nachenburg* to determine whether the memory regions are contiguous. Applicant further requests that the Examiner produce a reference in support of his position pursuant to M.P.E.P. § 2144.03.

Because Applicant believes he has amply demonstrated the allowability of the independent claims over the reference of the rejection, and to avoid burdening the record, Applicant has not provided detailed remarks concerning these dependent claims. Applicant, however, remains ready to provide such remarks if it becomes appropriate to do so. Accordingly, for at least the same reasons, Applicant also respectfully requests reconsideration and allowance of the claims that depend on independent Claims 1-2, 7-12, and 17-18.

**CONCLUSION**

Applicant has made an earnest attempt to place this case in condition for allowance. For at least the foregoing reasons, Applicant respectfully requests full allowance of all the pending claims.

If the Examiner believes a telephone conference would advance prosecution of this case in any way, the Examiner is invited to contact Keiko Ichiye, the Attorney for Applicant, at the Examiner's convenience at (214) 953-6494.

Although Applicant believes no fees are due, the Commissioner is hereby authorized to charge any fees or credit any overpayments to Deposit Account No. 02-0384 of Baker Botts L.L.P.

Respectfully submitted,

BAKER BOTTS L.L.P.  
Attorneys for Applicant



Keiko Ichiye  
Reg. No. 45,460

KI/lis

**Correspondence Address:**

Baker Botts L.L.P.  
2001 Ross Avenue, Suite 600  
Dallas, Texas 75201-2980  
(214) 953-6494  
Date: December 29, 2005

**Customer Number: 05073**